

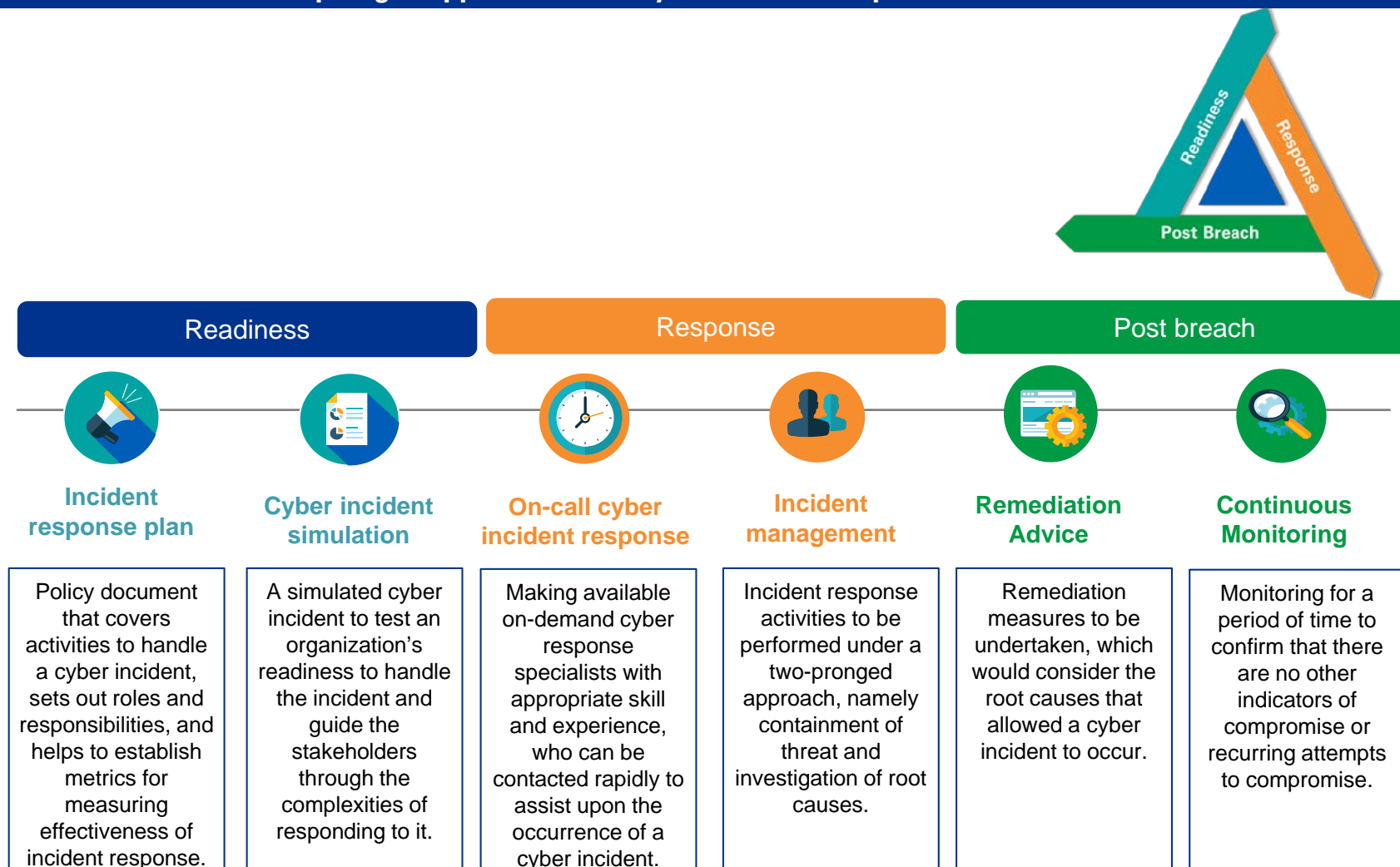


# An Introduction to KPMG's Cyber Response Services



# Cyber Response Services Overview

Our three pronged approach of the Cyber Incident Response is as set out below:



# Cyber Response Services

## Readiness

### 1. Cyber Response: Readiness Assessment

#### Incident Response Plan

While it is not possible to predict **when** the next cyber incident is going to happen, you can build controls to enable you respond to it effectively. A crucial control in this regard is an **Incident Response Plan**, which is a **primary reference document** to **define roles and responsibilities** of different stake holders during an incident management, and give guidance on **how to undertake which activities to respond and recover**.

##### People

- Critical decision makers
- Requisite training and skillsets



##### Processes

- Incident response steps
- Key processes defined
- Internal vs external communications



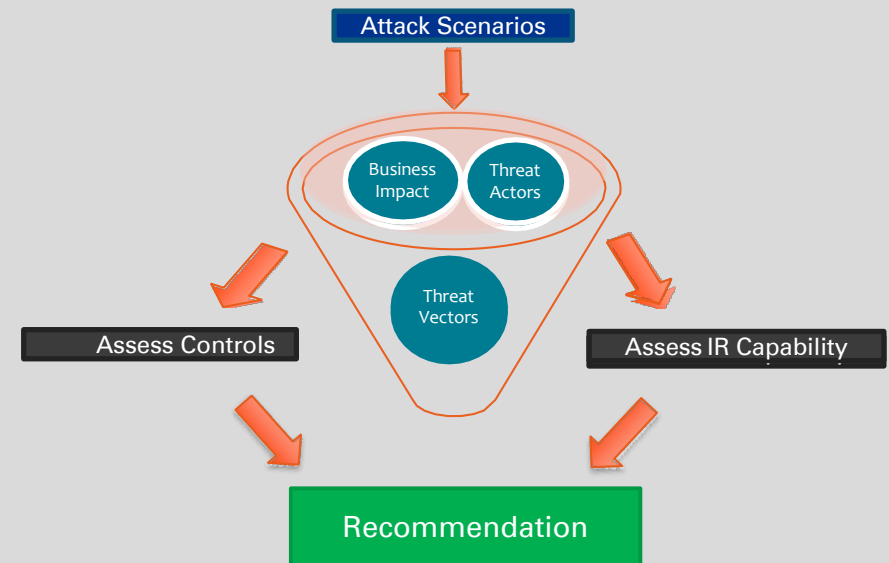
##### Technology

- Location of data
- Extraction of data
- Legal considerations
- Requisite analysis tools



#### Cyber Incident Simulation

To obtain an understanding of the bank's readiness on cyber response, a cyber incident simulation is an experiential exercise that will uncover operational issues. A facilitator walks through a **tailored cyber incident** with the group in stages, presenting key decision moments and works with the group, to **evaluate options and make decisions**, exposing key individuals to **real life challenges** of handling a cyber incident.

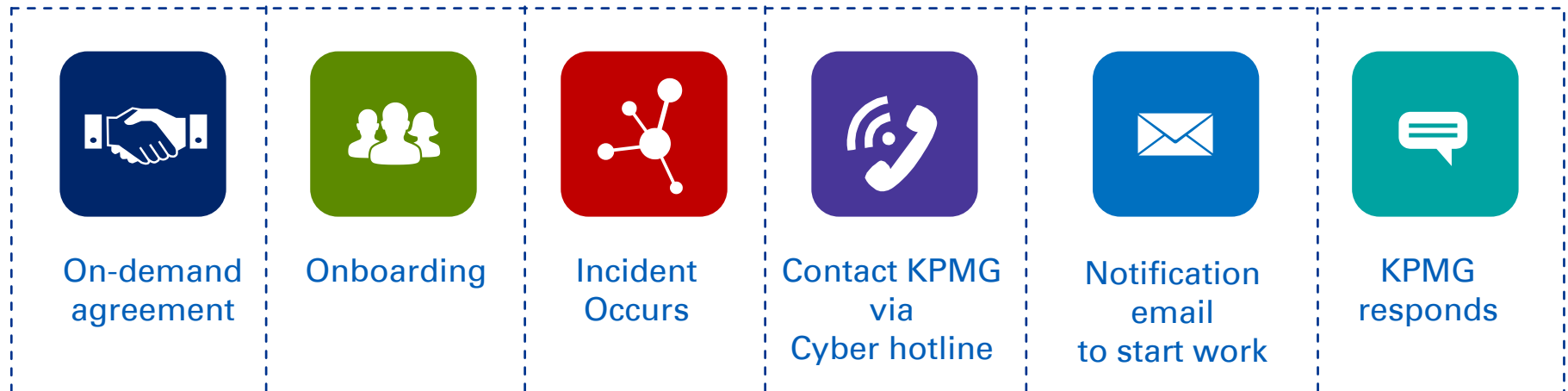


# Cyber Response Services

## Response

### 2. Cyber Response: On Call Services

KPMG's On-Call Cyber Incident Response Services model is a custom-tailored service for our Clients, which helps in ensuring an effective and faster response to the cyber incidents. The onboarding exercise helps KPMG gain a prior understanding of the Clients' IT environment and testing remote access mechanisms, if necessary. It is a highly flexible model, which can also be integrated with an Attorney Client Privilege or a Cyber Insurance Model.



#### Key Differentiators

- Easy contracting
- Optionally, no retainer
- Integration with Cyber Insurance Model, if necessary
- Accelerated Response Times either in Person or Remotely
- Hit the ground running with onboarding
- Amenable to Legal Privilege
- Technology agnostic

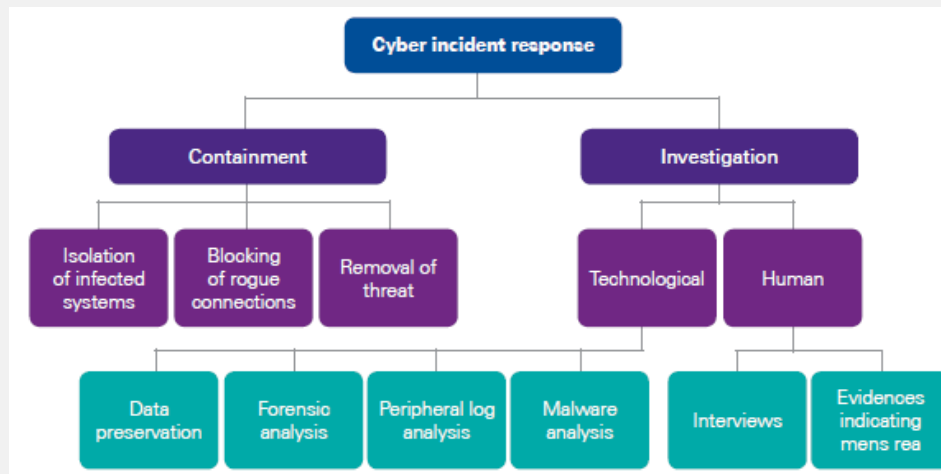
# Cyber Response Services

## Response

### 2. Cyber Response: Incident Management

Cyber incident management is a dynamic set of actions to handle a cyber security breach in a timely manner. There is a need to **respond effectively and efficiently** to cyber incidents, conducting technical analysis and identify effective mitigation measures.

Incident response should be conducted under a two-pronged approach, namely **containment** of threat and **investigation** of root cause. Considering the complexities associated with a cyber incident, the aforesaid two approaches may run simultaneously.



A typical incident investigation work flow is as given below:



# Cyber Response Services

## Post-Breach - Remediation Advice & Continuous Monitoring

### 3. Cyber Response: Post Breach

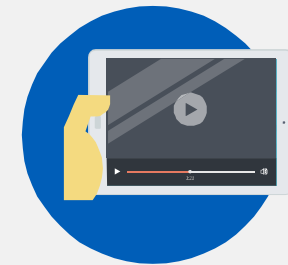
There are two key aspects, which should be considered subsequent to a cyber incident:

#### Remediation Advice

To prevent recurrence of cyber incidents in the future, a series of remediation measures should be undertaken, which would consider **the root causes** that allowed a cyber incident to occur. E.g. Phishing Emails, Brute Force/ Password Spraying Attacks, Zero Day Payloads, Exploitation of unpatched OS/ Application vulnerabilities, poor IT change management and Smoke Screens, among others.

#### Continuous Monitoring

To confirm that there are no other indicators of compromise ('IOC') or the recurring attempts to compromise, continuous monitoring of the compromised systems/ subnets/ IT environment should be performed subsequent to a cyber incident for a limited period of time.





# Overview of our forensic practice and select team members



# Overview of our forensic practice

KPMG has been in Hong Kong SAR since 1945 and was the first international accounting firm to be granted a foreign joint venture license in China in 1992. KPMG China has some 9,500 staff located across China. Our professionals provide services to a large and diversified portfolio of clients, including many of the leading public companies, multi-national companies, financial institutions, government authorities and public sector organizations.

- Forensic practice in the region was established in Hong Kong SAR in 1992 and in mainland China in 2004.
- Our client base is made up of numerous different entities, including multinational companies, local enterprises and government departments.
- We provide a wide range of Forensic services ranging from Fraud Risk Management to Forensic technology services.
- Our team is comprised of over 100 local and expatriate professionals based in Hong Kong, Shanghai and Beijing.
- Our individuals have a wide range of qualifications and backgrounds in accounting, technology, law, law enforcement, corporate intelligence, etc.
- We routinely work together with KPMG's International Forensic network to deliver our services to inbound and outbound investors in China. We have a staff rotation program with major overseas Forensic practices such as the United States, United Kingdom and Australia.



**Paul Pu**  
**Partner, Forensic**  
**Head of Forensic China & Hong Kong**  
+86 (21) 2212 3780  
paul.pu@kpmg.com



**Dakai Liu**  
**Partner, Forensic Shanghai**  
+86 (21) 2212 3371  
dakai.liu@kpmg.com



**Clark Zhu**  
**Partner,**  
**Head of Forensic, Beijing**  
+86 (10) 2212 3699  
clark.zhu@kpmg.com



Select Relevant  
Experience



# Select Relevant Experience - Cyber Response

We present below a select list of credentials in relation to cyber incident response:

<b>A Hong Kong based retailer</b>	<p>Hong Kong based company had its refrigeration system shutdown due to its ICS being manipulated. KPMG was appointed to identify the source of breach and the perpetrator who manipulated the ICS to shutdown the systems.</p> <p>The incident response included understanding of the working of the ICS and various logs capturing access to the system. During the course of investigation we learned system administrator had configured the ICS to turn to alternate supply mode with supply of 15 mins if anyone other than him tried to enter his cabin. This supply would trigger back to power only if you turned back the switch which was only know to him</p>
<b>A Philippines based Company</b>	<p>A Company in Philippines had its entire sub network encrypted by Ransomware, which contained important customer information. KPMG assisted the client by prioritising isolating of the servers, triaged the infected systems, monitored the security of the network.</p> <p>We also performed log analysis, host based forensics and implemented proactive monitoring of suspicious IP addresses which enabled us to get the critical evidence for analysis. The client was also involved the legal counsel for regulatory require for data exfiltration.</p> <p>Investigation of the ransomware behaviour was performed in KPMG's forensic lab in a sandbox environment. Payload signatures were shared with client to scan across network to identify if another systems were compromised.</p>
<b>A Hong Kong based technology company</b>	<p>A technology company in Hong Kong were victims of a wire transfer fraud as a result of an office365 email account breach.</p> <p>We were commissioned to understand what went wrong and the procedures to take in order to prevent the incident from happening again. Based on the request, we analysed email metadata, logs, and discovered how the attackers carefully manipulated the email flow to socially engineer the finance team to make payments to an unknown bank account.</p> <p>Through the investigation, we have identified that multiple accounts were compromised using a phishing link to an external cloud storage website. As an immediate remediation, we recommended IT team to block emails from suspicious IP identified during our investigation and implement multiple factor authentication for the email accounts.</p>

# Select Relevant Experience - Cyber Response (cont'd)

<b>Financial institution in Nepal</b>	<p>The electronic transaction system of the client was compromised by an attacker who performed unauthorised NEFT and RTGS transactions. The client requested KPMG to conduct a fact finding investigation to identify the root cause and the associated modus operandi. KPMG performed the following procedures:</p> <ul style="list-style-type: none"> <li>• Review of the digital footprints associated with the unauthorized transactions</li> <li>• Forensic acquisition and review of electronically stored information</li> <li>• Analysis of network logs during the period of review</li> <li>• Web server log analysis, forensic acquisition and malware analysis performed to identify the compromised systems.</li> </ul> <p>A detailed reverse engineering of the digital foot prints of the Trojan revealed the attack was initiated by an insider. Further action against employee initiated by the Client.</p>
<b>A large exchange in Kuwait City</b>	<p>The Client noticed that unauthorized financial transactions were made by obtaining wrongful access to its login credentials and the client suspected that an Advanced Persistent Threat may have been responsible for the breach of its IT security. As part of the response, KPMG performed the following:</p> <ul style="list-style-type: none"> <li>• Forensic preservation and analysis of electronically stored information from mail server and end point machines used for carrying out financial transactions</li> <li>• Analysis of peripheral logs</li> <li>• Cyber security review of the Client's IT infrastructure connected or related to the unauthorized financial transactions</li> </ul> <p>We identified a backdoor, which was connected to a rogue IP address having a geo-location of an East European Nation, identified internet explorer password grabbers and other customised malware used for carrying out a targeted attack and identified systemic vulnerabilities, which potentially led to the cyber heist. Specific recommendations were provided to remediate the above.</p>
<b>An automobile manufacturing company</b>	<p>We were engaged by an automobile manufacturing company with substantial market share in India, and having significant exports across Asia, Europe, etc. to investigate a number of ransomware attacks. As part of the response plan, KPMG assisted the client with the following:</p> <ul style="list-style-type: none"> <li>• Forensic analysis of infected systems</li> <li>• RCA using system files, event logs, e-mails, web browser</li> <li>• Reverse engineering of identified malicious file sin a controlled sandboxed environment</li> <li>• Assistance in remediation</li> </ul> <p>As a result of our work, we blocked malicious files from causing infection on other machines, identified the root case of the malware infection and blocking o the command and control server IP address at the network level and provided recommendations for strengthening the IT environment.</p>



[kpmg.com/socialmedia](https://kpmg.com/socialmedia)

© 2020 KPMG Advisory (Hong Kong) Limited, a Hong Kong entity and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Hong Kong.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

This capability statement is made by KPMG Advisory (Hong Kong) Limited, a Hong Kong entity and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity, and is in all respects subject to the negotiation, agreement and signing of a specific engagement letter or contract and subject to the completion of customary client acceptance procedures. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.